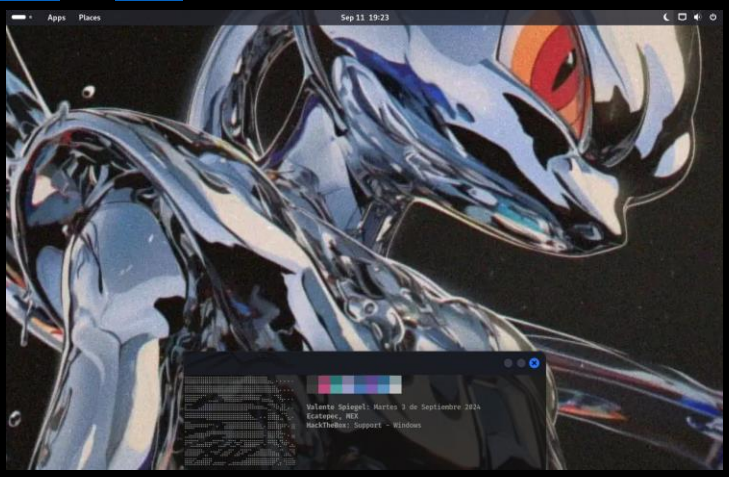
Ethical hacking lab: Support HackTheBox

"Mi intención, además de llevar un Conteo y Evidencia de mi progreso en la formación como Pentester, es despertar la curiosidad en la comunidad mexicana y de habla hispana sobre temas de Hacking Ético. Quiero ofrecer lo que considero una explicación 'sencilla' de lo complejo y fascinante que son los sistemas vulnerables en la actualidad."

/▲\ Correo /▲\ tiktok /▲\ github



Atacante ---------- |10.10.19.30|

|>/////////// Linux|

Victima ---------- |10.10.11.130|

|> /////// Windows|

Walkthrough

| 1 | Enumeración de Servicios y Descubrimiento

Iniciamos nuestra evaluación de la red con un simple comando ping, obteniendo una respuesta con un TTL=127, lo que indica que estamos tratando con un entorno Windows. Luego, utilizamos Nmap para escanear puertos y servicios, descubriendo varias tecnologías en uso. Nos centramos en el puerto 445, típicamente utilizado por los servicios SMB. Con la herramienta smbclient, accedemos a los recursos compartidos sin necesidad de autenticación, y encontramos el directorio 10.10.11.17//support-tools, que parece estar destinado al equipo de soporte técnico.

| 2 | Identificación del Domain Controller.

Antes de profundizar, determinamos el nombre del Domain Controller (DC). El escaneo previo con Nmap ha indicado que el entorno utiliza Active Directory. Utilizamos crackmapexec, que nos revela el nombre del DC como support.htb. Añadimos este nombre al archivo /etc/hosts, anticipando que los servicios en este laboratorio puedan estar configurados con virtual hosting.

| 3 | Explotacion

En el directorio 10.10.11.17//support-tools, encontramos varias herramientas de soporte técnico, como PuTTY y 7-Zip. Sin embargo, el archivo Usersinfo.exe.zip nos llama la atención. Descomprimimos el archivo y encontramos el ejecutable userInfo.exe. Usamos dnSpy para depurar el binario, buscando posibles vulnerabilidades en la sanitización del código. Al analizar el comportamiento en memoria, descubrimos el hash del usuario ldap. Usamos ldapsearch para realizar una enumeración LDAP y revelamos información sensible, incluyendo una contraseña en texto claro. Finalmente, intentamos autenticarnos con winrm utilizando las credenciales descubiertas, obteniendo una consola interactiva como el usuario support.

Ethical hacking lab: Support HackTheBox

Habilidades.

TTL (Time To Live)

- **Qué es**: Es un campo en el encabezado de un paquete IP que especifica el número máximo de saltos que el paquete puede hacer en la red antes de ser descartado.
- **Para qué sirve**: Evita que los paquetes se queden atrapados en bucles de red infinitos y ayuda a limitar la propagación de paquetes dañinos o no deseados.

Servicio SMB (Server Message Block)

- **Qué es**: Es un protocolo de red utilizado para compartir archivos, impresoras y otros recursos en una red.
- **Para qué sirve**: Permite a los programas en un computador acceder a archivos y recursos en otros computadores a través de una red local o en la red de área amplia (WAN).

smbclient

- **Qué es**: Es una herramienta de línea de comandos para acceder a recursos compartidos de SMB/CIFS.
- **Para qué sirve**: Permite explorar y manipular recursos compartidos en servidores que usan el protocolo SMB, como compartir archivos y directorios.

Domain Controller (DC)

- **Qué es**: Es un servidor en una red de Windows que maneja la autenticación y autorización de usuarios y equipos.
- **Para qué sirve**: Administra y autentica las credenciales de los usuarios y controla el acceso a recursos de la red dentro de un dominio de Active Directory.

Active Directory (AD)

- **Qué es**: Es un servicio de directorio desarrollado por Microsoft para redes Windows.
- **Para qué sirve**: Proporciona servicios de autenticación y autorización, organiza los recursos de red (usuarios, grupos, equipos) en una estructura jerárquica, y gestiona políticas y permisos en una red empresarial.

crackmapexec

- **Qué es**: Es una herramienta de pentesting y administración de red que permite la enumeración y explotación de redes Windows.
- **Para qué sirve**: Facilita la interacción con servicios como SMB, Kerberos, y otros protocolos de red para realizar auditorías de seguridad y obtener información sobre los sistemas.

Virtual Hosting

- **Qué es**: Es una técnica de hosting que permite a un solo servidor alojar múltiples dominios o sitios web.
- **Para qué sirve**: Optimiza el uso de recursos y permite la gestión de varios sitios web en un solo servidor, con cada sitio operando como si tuviera su propio servidor dedicado.

Vulnerabilidades de Sanitización

- **Qué es**: Son fallos en el manejo de datos que permiten la entrada de datos maliciosos en un sistema.
- **Para qué sirve**: La falta de sanitización adecuada puede llevar a ataques como inyecciones de código, que pueden comprometer la seguridad de una aplicación o sistema.

Ethical hacking lab: Support HackTheBox

dnSpy

- **Qué es**: Es una herramienta de decompilación y depuración para aplicaciones .NET.
- **Para qué sirve**: Permite analizar, depurar y modificar el código de aplicaciones .NET, facilitando el análisis de vulnerabilidades y la ingeniería inversa.

LDAP (Lightweight Directory Access Protocol)

- **Qué es**: Es un protocolo para acceder y mantener servicios de directorio distribuidos sobre una red.
- **Para qué sirve**: Permite la autenticación y la consulta de datos de directorio, como información de usuarios y grupos, en redes corporativas.

ldapsearch

- **Qué es**: Es una herramienta de línea de comandos para consultar un servidor LDAP.
- **Para qué sirve**: Permite realizar búsquedas en un directorio LDAP, obteniendo información sobre las entradas y atributos almacenados en el directorio.

LDAP Enumeration

- **Qué es**: Es una técnica para extraer información de un servidor LDAP.
- **Para qué sirve**: Permite descubrir detalles sobre usuarios, grupos y otros objetos en un directorio LDAP, lo que puede ser útil para auditorías de seguridad y pruebas de penetración.